

CLAIMS

WE CLAIM:

1. A method of authenticating a principal in a network environment for access to secured resources comprising:

receiving at an authority a login request from the principal, wherein the login request comprises an account identifier;

transmitting the account identifier from the receiving authority to a super authority for identification of an authority that is authorized to authenticate the principal;

and

authenticating the principal at the receiving authority if a transmission is received at the receiving authority from the super authority indicating that the receiving authority is authorized to authenticate the principal, and otherwise abstaining from authentication of the principal.
2. The method according to claim 1, wherein the account identifier comprises a principal identifier and a namespace identifier.
3. The method according to claim 1, further comprising:

receiving at the receiving authority from the super authority a request to authenticate a second principal based on a login request made by the second principal, wherein the login request made by the second principal was made by the requesting principal to another authority other than the receiving authority.

4. A controlling authority for identifying an authenticating authority for authenticating a principal for access to network resources comprising:

an identity catalog mapping at least one account ID of at least one principal to an identifier of a corresponding authenticating authority; and

an authority resolution module for accessing the identity catalog to match the account ID with a corresponding authenticating authority and for causing an authentication request to be directed to the corresponding authenticating authority.

5. The controlling authority according to claim 4, further comprising a network interface for passing the account ID to the authority resolution module and for receiving from the authority resolution module an authentication request directed to the corresponding authenticating authority.

6. The controlling authority according to claim 4, wherein the identity catalog maps a plurality of account IDs to a corresponding plurality of authenticating authorities.

7. The controlling authority according to claim 6, wherein each account ID comprises a namespace identifier, and wherein the plurality of account IDs comprises at least two account IDs having a common namespace identifier, wherein the at least two account IDs are mapped to at least two different respective ones of the plurality of authenticating authorities.

8. The controlling authority according to claim 6, wherein each account ID comprises a namespace identifier, and wherein the plurality of account IDs comprises at least two account IDs having different namespace identifiers, wherein the at least two account IDs are mapped to the same one of the plurality of authenticating authorities.

9. The controlling authority according to claim 6, wherein the content of the identity catalog is based at least in part on the organizational affiliation of principals within an entity.

10. The controlling authority according to claim 6, wherein the content of the identity catalog is based at least in part on the geographical location of principals.

11. A method of controlling authentication of principals for access to network resources in a network environment comprising:

receiving a request for an authenticating authority resolution from one of a plurality of authenticating authorities, wherein the request comprises an account ID of a principal to be authenticated;

accessing an assignment mapping of a plurality of account IDs to a corresponding plurality of authenticating authorities and locating within the mapping the account ID of the principal to be authenticated;

locating within the mapping an identity of an assigned authenticating authority that is mapped to the account ID of the principal to be authenticated; and

causing an authentication request to be transmitted to the assigned authenticating authority, wherein the request asks the assigned authenticating authority to authenticate the principal to be authenticated.

12. The method according to claim 11, wherein each account ID comprises a namespace identifier, and wherein the plurality of account IDs comprises at least two account IDs having a common namespace identifier, wherein the at least two account IDs are mapped to at least two different respective ones of the plurality of authenticating authorities via the assignment mapping.

13. The method according to claim 11, wherein each account ID comprises a namespace identifier, and wherein the plurality of account IDs comprises at least two account IDs having different namespace identifiers, wherein the at least two account IDs are mapped to the same one of the plurality of authenticating authorities via the assignment mapping.

14. The method according to claim 11, further comprising altering the assignment mapping whereby an account ID previously mapped to a first authenticating authority is remapped to a second authenticating authority.

15. The method according to claim 11, wherein the assignment mapping is based at least in part on the organizational affiliation of principals within an entity.

16. The method according to claim 11, wherein the assignment mapping is based at least in part on the geographical location of principals.

17. An apparatus for controlling authentication of principals for access to network resources in a network environment comprising:

means for receiving a request for an authenticating authority resolution from one of a plurality of authenticating authorities, wherein the request comprises an account ID of a principal to be authenticated;

means for accessing an assignment mapping of a plurality of account IDs to a corresponding plurality of authenticating authorities and for locating within the mapping the account ID of a principal to be authenticated;

means for locating within the mapping an identity of an assigned authenticating authority that is mapped to the account ID of a principal to be authenticated; and

means for causing an authentication request to be transmitted to the assigned authenticating authority, wherein the request invites the assigned authenticating authority to authenticate the principal to be authenticated.

18. The apparatus according to claim 17, wherein each account ID comprises a namespace identifier, and wherein the plurality of account IDs comprises at least two account IDs having a common namespace identifier, wherein the at least two account IDs are mapped to at least two different respective ones of the plurality of authenticating authorities via the assignment mapping.

19. The apparatus according to claim 17, wherein each account ID comprises a namespace identifier, and wherein the plurality of account IDs comprises at least two account IDs having different namespace identifiers, wherein the at least two account IDs are mapped to the same one of the plurality of authenticating authorities via the assignment mapping.

20. The apparatus according to claim 17, further comprising means for altering the assignment mapping whereby an account ID previously mapped to a first authenticating authority is remapped to a second authenticating authority.

21. A computer-readable medium having thereon computer-executable instructions for performing a method of controlling authentication of principals for access to network resources in a network environment comprising the steps of:

receiving a request for an authenticating authority resolution from one of a plurality of authenticating authorities, wherein the request comprises an account ID of a principal to be authenticated;

accessing an assignment mapping of a plurality of account IDs to a corresponding plurality of authenticating authorities and locating within the mapping the account ID of a principal to be authenticated;

locating within the mapping an identity of an assigned authenticating authority that is mapped to the account ID of a principal to be authenticated; and

causing an authentication request to be transmitted to the assigned authenticating authority, wherein the request asks the assigned authenticating authority to authenticate the principal to be authenticated.

22. The computer-readable medium according to claim 21, wherein each account ID comprises a namespace identifier, and wherein the plurality of account IDs comprises at least two account IDs having a common namespace identifier, wherein the at least two account IDs are mapped to at least two different respective ones of the plurality of authenticating authorities via the assignment mapping.

23. The computer-readable medium according to claim 21, wherein each account ID comprises a namespace identifier, and wherein the plurality of account IDs comprises at least two account IDs having different namespace identifiers, wherein the at least two account IDs are mapped to the same one of the plurality of authenticating authorities via the assignment mapping.

24. The computer-readable medium according to claim 21, wherein the assignment mapping is based at least in part on the organizational affiliation of principals within an entity.

25. The computer-readable medium according to claim 21, wherein the assignment mapping is based at least in part on the geographical location of principals.